INDIA'S AADHAAR CARD – A VIOLATION OF INDIAN CITIZEN'S RIGHT TO PRIVACY

Sonal Chhugani[†]

TABLE OF CONTENTS

I. INTRODUCTION

India—a nation with over twenty-two national languages, a myriad of cultures and religions, and 1.2 billion citizens—is one of the most diverse and dynamic countries on the planet.[1] Already hailed the

[†] Note Editor of Cardozo International and Comparative Law Review; Vice President of Cardozo's South Asian Law Students Association; B.A. in Individualized Studies, concentrating in Producing and Theatrical Management for the South and

"largest democracy in the world" due to its sheer size, India's population continues to grow exponentially.[2] This rapid growth, poses regulatory concerns for a government that is already facing problems both with the distribution of benefits and with corruption.[3] Therefore, to alleviate these problems, India introduced a new national identification card system—the Aadhaar Card.[4]

The Aadhaar Card is a mandatory national identification card system that provides Indian citizens with a unique identification number.[5] In order to receive the card, citizens need to provide a large amount of personal information, including biometric and demographic data.[6] This information is stored in one centralized database that is governed by a single government entity.[7] As such, many Indian citizens are concerned with the security and usage of their personal data as it relates to their fundamental right to privacy.[8] In order to extinguish these fears, the issue was brought forward to the Indian judiciary.[9] However,

---

East Asian region, from New York University's Gallatin School of Individualized Studies. A special thank you to my parents, Sunil and Deepika Chhugani, along with my friends and colleagues, Alison, Daniel and Mendel, for your tremendous love and support throughout law school.

1 *Culture Map of India*, MAPS OF INDIA (Nov. 27, 2017), https://www.mapsofindia.com/culture/; *The World Bank in India*, THE WORLD BANK, https://www.worldbank.org/en/country/india (last visited Feb. 7, 2020).

2 *The World Bank in India*, *supra* note 1; Hannah Ritchie, *India's Population Growth Has Come to an End: The Number of Children Has Already Peaked*, OUR WORLD IN DATA (Jan. 15, 2019), https://ourworldindata.org/indias-population-growth-will-come-to-an-end.

3 Anviti Chaturvedi, *Overview of the Legal Issues Around Aadhaar*, PRS LEGISLATIVE RESEARCH (Sept. 11, 2019), http://www.prsindia.org/theprsblog/overview-legal-issues-around-aadhaar; Reetika Khera, *These digital IDs have cost people their privacy – and their lives*, WALL ST. J. (Aug. 9, 2018), https://www.washingtonpost.com/news/the-worldpost/wp/2018/08/09/aadhaar/; Caroline E. McKenna, *India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System*, 38 BROOK. J. INT'L L. 729 (2013).

4 Chaturvedi, *supra* note 3; Rahul Bhatia, *The Indian Government's Astonishing Hunger for Citizen Data*, N.Y. TIMES (Oct. 5, 2018), https://www.nytimes.com/2018/10/05/opinion/india-supreme-court-biometrics.html.

5 Chaturvedi, *supra* note 3.

6 *Id.*

7 *Id.*

8 *Id.*

9 *Id.*; *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, PRIVACY INT'L (Sept. 11, 2019), https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar.

in 2018, the Indian Supreme Court ruled that the Aadhaar Card does not violate an Indian citizens right to privacy under the Indian Constitution.[10]

Hence, this note looks to determine whether Indian citizens have an alternative route of recourse through India's international treaty obligation under the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR provides that human beings have a fundamental right to privacy, and that states must protect that right.[11] Consequently, this note analyzes whether India's Aadhaar Card program is in compliance with the right outlined in Article 17 of the ICCPR, and if not, recommends amendments to the program and the likelihood of its enforcement.

As such, Part II of this note will set the landscape of the Aadhaar Card program by first providing a detailed description of the Aadhaar Card system and the concerns surrounding its usage. Part II will also analyze the right to privacy under Indian constitutional law and the final ruling that determined that the Aadhaar Card was not in violation of this constitutional right.

Part III will then look to India's international treaty obligation under the ICCPR. It will first define the right to privacy under Article 17 of the ICCPR and will then outline how this right applies in our modern digital age.

Subsequently, Part IV will analyze whether the Aadhaar Card program violates Article 17 of the ICCPR as described in Part III. Since the inquiry reveals that the system indeed does violate the right to privacy under the ICCPR, Part V of the note presents recommendations for amendments to the Aadhaar Card program and particular methods of enforcing compliance.

Finally, Part VI provides a conclusion to the arguments and proposal.

---

10 *Initial Analysis of Indian Supreme Court decision on Aadhaar*, *supra* note 9.

11 G.A. Res. 2200A (XXI), Int'l Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

II. THE AADHAAR CARD

A. Introduction to the Card and It's Processes

India is home to 1.2 billion citizens, making its population the second largest in the world.[12] Given the country's enormous size, the Indian government has been confronting challenges with regards to the regulation of the distribution of benefits.[13] Previously, various benefits, such as driver's licenses, voter identification cards, and ration cards, required different types of identity proof.[14] However, for those living in poverty, these forms of identification were difficult to attain and could be readily reproduced.[15] Forged documents, along with the help of corrupt government employees, made benefiting from another's government services and subsidies effortless.[16] As the population of India continues to grow, in order to resolve this issue and prevent exacerbation of this problem, the government of India initiated the "Aadhaar Project."[17]

The Aadhaar Project was initiated as a voluntary program in 2009 to provide individuals with a more reliable "biometric-based unique identity number."[18] In order to receive an identification card that contains the unique identity number, individuals have to submit biometric data, such as fingerprints and iris scans, along with demographic information, such as their date of birth and gender.[19] A decade ago, the program was completely voluntary.[20] Individuals could evaluate the costs and benefits of participating before making a choice. However, at the direction of Prime Minister Narendra Modi, the Indian government sought to make the Aadhaar Card mandatory for all Indian citizens.[21]

The Indian Parliament passed the Aadhaar Act in 2016, requiring all citizens to obtain the Aadhaar Card.[22] The Act gave legislative

12 *The World Bank in India*, *supra* note 1.
13 Chaturvedi, *supra* note 3; Khera, *supra* note 3; McKenna, *supra* note 3, at 729.
14 Chaturvedi, *supra* note 3.
15 *Id.*; McKenna, s*upra* note 3, at 730.
16 Chaturvedi, *supra* note 3.
17 *Id.*; Bhatia, *supra* note 4.
18 Chaturvedi, *supra* note 3; Bhatia, *supra* note 4.
19 Chaturvedi, *supra* note 3.
20 Bhatia, *supra* note 4.
21 *Id.*
22 Chaturvedi, *supra* note 3.

authorization to government bodies and private companies to use the Aadhaar Card as their main required source of identification.[23] As a result, the Aadhaar Card was utilized in every facet of an individual's life.[24] For example, the unique identification number was required to certify marriages, receive welfare and pension payments, purchase cellular service, and open bank accounts.[25] The following year, the Indian Parliament amended the Income Tax Act to the Finance Act, requiring citizens to use their Aadhaar identification number to receive their tax identification numbers and file their tax returns.[26] The Aadhaar Card, which translates to "foundational card" in English, truly began to emulate its meaning.[27]

While this outcome is a great victory for the Indian government, it causes great concern for the general population. Each individual's biometric data, demographic information, bank account number, tax returns, marriage certificates, cellular number, pension benefits, and welfare payments, are connected to one singular unique identification number, which is stored in one centralized database.[28] This centralized database is administrated by one single government agency, the Unique Identification Authority of India (UIDAI).[29] The connection of all of these individual silos of data in one concentrated location, brings forth immense concerns over data security, government profiling, and surveillance.[30]

1. Data Security

When the Aadhaar Act was passed, the Indian Parliament knew that India "does not have comprehensive law on privacy and data security," and only included minimal protections against these concerns

---

23 *Id.*

24 Khera, *supra* note 3.

25 *Id.*

26 Chaturvedi, *supra* note 3.

27 Mishi Choudhary, *Viewpoint: The Pitfalls of India's Biometric ID Scheme*, BBC (Apr. 23, 2018), https://www.bbc.com/news/world-asia-india-43619944.

28 Khera, *supra* note 3.

29 Chaturvedi, *supra* note 3.

30 *Id.*; Bhatia, *supra* note 4; Reetika Khera, *Aadhaar Verdict: Big data Meets Big Brother*, LIVE MINT (Oct. 1, 2018), https://www.livemint.com/Politics/0LTYZzCHQb9X6UFsn09lBI/Aadhaar-verdict-big-data-meets-big-brother.html.

in the Act.[31] For instance, aside for lawfully authorized exceptions, the Act prohibits obtaining another's information without their consent, sharing biometric data with anyone other than the owner, publicly displaying a person's unique identification number, and explicit restrictions on government officers from sharing any personal information.[32] Yet, these safeguards are not enough, and citizens still believe that there are aspects of the Aadhaar Card scheme that gravely violate their privacy rights, or at least have incredible potential to cause them injury.[33]

As previously mentioned, one specific area of concern is the massive amount of data stored in one central location.[34] Indian journalist Reetika Khera writes:

> What sets Aadhaar apart from other examples where the state demands our data (say, the Registration Act or the Social Security Number) is that our biometric and demographic data are being stored in a centralized database and a unique number is associated with our biometric and other information. Further, this unique number was being seeded (added as a new data field) with every possible—public and private—database in the country.[35]

Many citizens worry that the government now has the ability to use their unique identification number to access all of their data without any prior authorization.[36] They assert that this fear is further aggravated by the lack of preexisting data privacy laws to protect their information from misuse.[37]

Without sufficient safeguards in place for data security, particularly because the data is being stored in one location, everyone's personal information is extremely vulnerable.[38] Unfortunately, these fears

---

31 Chaturvedi, *supra* note 3.

32 *Id.*

33 *Id.*

34 *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

35 *Id.*

36 *Id.*

37 McKenna, *supra* note 3, at 752.

38 Chaturvedi, *supra* note 3; *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

have already turned into reality.[39] Over one hundred cases of fraudulent activity have been reported, including the forging of Aadhaar Cards to open bank accounts, receive loans, and to steal money.[40] In order to investigate the difficulty of breaching Aadhaar Card data, the newspaper, *The Tribune India*, attempted to access other people's information.[41] The paper reports:

> Today, The Tribune "purchased" a service being offered by anonymous sellers over WhatsApp that provided unrestricted access to details for any of the more than 1 billion Aadhaar numbers created in India thus far. It took just Rs. 500, paid through Paytm, and 10 mins. in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. Lo and behold, you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code, photo, phone number and email.[42]

In reaction to this news, an UIDAI officer admitted that this was a "major national security breach."[43] Consequently, this raises severe concerns of identity theft and encumbrances of personal liberties.[44]

Citizens complete lack of control over their data causes understandable and continued anxiety.[45] While they are concerned with their inability to assert any power in regard to their own information, they are also apprehensive about others accessing their personal materials fraudulently.[46] Moreover, citizens state that their concerns with the central storage of Aadhaar information is a result of the great amount

---

39 Chaturvedi, *supra* note 3; *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

40 Chaturvedi, *supra* note 3; *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

41 Rachna Khaira, *Rs 500, 10 minutes, and You Have Access to Billion Aadhaar Details*, TRIBUNE (Jan. 4, 2018), https://www.tribuneindia.com/news/archive/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

42 *Id.*

43 *Id.*

44 *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

45 *Id.*

46 Chaturvedi, *supra* note 3.

of personal data that one could access by simply breaching the Aadhaar central database.[47] More importantly, stealing a unique identification number from the centralized database now provides a gateway to reach other personal information, such as bank account numbers and tax information.[48]

2. Profiling

Second, citizens fear that the card will incite further discrimination, as government officials are able to link personal traits that could indicate an individual's caste or race to the card.[49] In turn, this raises concerns that this practice will allow the government to construct a full 360-degree profile of each citizen, in turn using it to profile them.[50] While there is no proof that the government conducts this practice, "just the possibility of such profiling is likely to lead to self-censorship" and "stifle dissent."[51] In response to these concerns, UIDAI CEO Ajay Bhushan Pandey, has stated that "no one can build Aadhaar users' profile."[52] He explains that no agency that uses the Aadhaar identification number is able to attain access to the other transactions linked to the number, and hence, there can be no 360-degree view of any user.[53] However, citizens remain concerned. They say that Ajay Bhushan Pandey has misinterpreted "profiling."[54] Indian citizens say this is not only a violation of their privacy, but of their civil liberties as well.[55]

3. Surveillance

Lastly, Indian citizens are troubled by the idea that the centralized nature of the Aadhaar scheme could be used as a tool for

---

47 Khera, *supra* note 3.

48 *Id.*

49 McKenna, *supra* note 3, at 753.

50 *Id.*

51 *Id.*

52 *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

53 Mahendra Singh, *No One Build Aadhaar Users' Profile: UIDAI Chief*, TIMES OF INDIA (May 7, 2017), https://timesofindia.indiatimes.com/india/no-one-can-build-aadhaar-users-profile-uidai-chief/articleshow/58556043.cms.

54 *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

55 McKenna, *supra* note 3, at 753.

surveillance.[56] That is because every time someone uses their unique identification number in a transaction, the transaction is recorded in an authentication transaction log, which is handled by the UIDAI.[57] This means that the log contains "a list of all bank accounts, all uses of a health care system, all benefits at point of use."[58] Indian citizens are concerned that this information could be used to monitor their lives and movements, a form of surveillance.[59]

As such, many Indian citizens have attacked the Aadhaar Project as counter to the Constitution of India—they argue that the Aadhaar Project is a violation of their fundamental right to privacy.[60]

B. India's Right to Privacy and the Recent Indian Supreme Court Ruling

Much like the constitutions of other democratic nations, the Constitution of India outlines a number of fundamental rights owed to its citizens.[61] In Part III of the Constitution—also known as the Fundamental Rights section, specifically Articles 12 to 35, the Constitution guarantees basic freedoms, such as the right to equality, freedom of speech, right against exploitation, freedom of religion, and personal liberty.[62] The inclusion of these rights aligns with the intent held by the drafters of the Indian Constitution, who wrote the Constitution to "secure justice, liberty, and equality to the people of India."[63] However, clearly absent from these protections is the fundamental right to privacy.[64] One assumption would be that the framers of the Indian Constitution intentionally excluded a protection for privacy. Yet, Indian citizens assert that a right to privacy is within the privileges afforded to them by their constitution.[65] That is because in various cases,

---

56 *Id.*

57 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

58 *Id.*

59 McKenna, *supra* note 3, at 755.

60 Chaturvedi, *supra* note 3.

61 *Fundamental Rights*, KNOW INDIA, https://knowindia.gov.in/profile/fundamental-rights.php (last visited Oct. 26, 2020).

62 *Id.*; Madison Julia Levine, *Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States*, 73 U. MIAMI L. REV. 618, 622 (2019).

63 Levine, *supra* note 62, at 622.

64 *Id.* at 622-23.

65 *Id.* at 622.

the Supreme Court of India has ambiguously implied a right to privacy from Article 19 and 21 of the Indian Constitution, which state that citizens have a right to freedom of expression and personal liberty.[66]

Indian citizens asserting this right in courts have caused a flurry of opinions that were largely in conflict with one another.[67] This is because through Indian Supreme Court decisions "there was a general understanding of an implied right to privacy in India, but its boundaries remained imprecise."[68] The Indian Supreme Court adjudicated via a "case-by-case basis," resulting in a landscape where "no overarching principles existed to clarify what the legitimate countervailing interests to privacy are," and "no clear, objective, universal threshold standard" was available either.[69] Lower courts themselves were unsure of how to resolve issues involving privacy principles. This resulted in a lack of uniform protections for privacy in India until 2017, when the Indian Supreme Court decided the case of *Puttaswamy v. Union of India*.[70]

In *Puttaswamy v. Union of India*, the court firmly held that "an individual's right to privacy is an inherent part of the right to life and personal liberty, and therefore implied in Article 21 of the Indian Constitution."[71] An analysis conducted of the court's opinion states:

> The *Puttaswamy I* judgment recognized the importance and value of privacy as a constitutional entitlement, not through the process of amendment, but through judicial interpretation by determining the nature and the extent of the freedoms available to each person protected under the Indian Constitution. The Court looked to Article 21 to interpret and establish this fundamental right. Justice Chandrachud explained that the right to privacy is implicit in the right to life and liberty guaranteed to citizens by Article 21 and that citizens have a right to safeguard that privacy.[72]

---

66 Ujala Uppaluri & Varsha Shivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating Toward a Privacy Right in India*, 5 NUJS L. REV. 21, 42 (2016).

67 Levine, *supra* note 62, at 623.

68 *Id.* at 622.

69 Uppaluri & Shivanagowda, *supra* note 66, at 44.

70 *Id.*

71 *Id.*

72 *Id.*

Even though *Puttaswamy v. Union of India*, firmly established a fundamental right to privacy, the right was largely regarded as one in relation to personal and domestic circumstances.[73] Data privacy, involved in economic and technological transactions, was typically viewed as a matter of self-regulation governed by a piecemeal statutory framework that provides minimal protections.[74] As such, controversies surrounding the Aadhaar Card continued to ensue.

In response, in 2018 the Supreme Court of India made its decision on whether the Aadhaar Card violated citizens' constitutional right to privacy.[75] In a 1448-page judgment, the Court ruled that the Aadhaar Card does not violate citizens' constitutional right to privacy, as there are "sufficient measures in place to protect data" and "it is difficult to undertake surveillance of citizens on the basis of Aadhaar."[76]

In order to reach its holding, the Court had to conduct a proportionality test in which a measure restricting a right must be narrowly tailored to a legitimate goal, and "the social or public interest and the reasonableness of restrictions outweigh the particular" intrusions onto that right.[77] The Court found that the state had a legitimate purpose to "ameliorate the sufferings of the downtrodden" by ensuring "that these [government] benefits actually reach the populace for whom they are meant."[78] Furthermore, the Court stated that the means for achievement are rationally related to the goal, and no other measure could be adopted that would attain the same results.[79] Additionally, the measure taken is narrowly tailored, since the information collected for enrollment in the program is minimal.[80] Hence, when balancing the public interest, which here is the dignity for the unprivileged conducted through better living standards, with the minimal privacy invasion, the Aadhaar Act passes the test.[81]

Justice Chandrachaud dissented from the opinion, as he found "that the legitimate aim of the State can be fulfilled by adopting less intrusive measures as opposed to the mandatory enforcement of the

---

73 McKenna, *supra* note 3, at 739.
74 *Id.*
75 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.
76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

Aadhaar scheme as the sole repository of identification."[82] His dissent identified four main weaknesses in the Aadhaar system.[83] First, the UIDAI necessitates accountability and redress mechanisms for data protection.[84] Second, the Aadhaar system has not tackled the issue of data security.[85] Third, the Aadhaar system does not prevent private entities from using the Aadhaar identification system in their practices, as they could exploit personal data for commercial purposes.[86] Moreover, by linking the unique identification number to private services, future profiling is a strong possibility, if data collection records show a person's preferences and selection of services.[87] Justice Chandrachaud notes that this could lead to self-censorship.[88] Fourth, the mandatory nature of the Aadhaar system makes it "impossible to live in contemporary India without Aadhaar," which is an overbreadth of the system.[89]

In line with some of the concerns raised in the dissent, despite upholding the Aadhaar Card's general constitutional validity, the majority did strike down certain uses of the system.[90] After the ruling, the Aadhaar Card can no longer be used by telecommunication companies as a source of identification for obtaining SIM cards.[91] The Court stated that "the conflation of biometric data with SIM cards is replete with grave dangers to personal autonomy," and "a constitution based on liberal values cannot countenance an encroachment of this nature."[92] Additionally, banks are not allowed to require Aadhaar cards as prerequisites to opening bank accounts; education entities and state administered examinations cannot make the Aadhaar Card

---

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

87 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

88 *Id.*

89 *Id.*; Gautum Bhatia, *Two Arguments Against the Constitutionality of Section 66A*, THE CENTRE FOR INTERNET & SOCIETY (May 31, 2014), https://cis-india.org/internet-governance/blog/two-arguments-against-the-constitutionality-of-section-66a (overbreadth is when a statute includes within its prohibitions conduct that it is entitled to prohibit, as well conduct that it is not).

90 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

91 *Id.*

92 *Id.*

compulsory for admission; and private entities are banned from asking for Aadhaar information.[93]

In addition to restrictions on certain uses of the Aadhaar Card, the Court restricted the government from making changes to the Aadhaar system.[94] In order to better protect privacy, the Court changed the allowable information retention period from five years to six months.[95] Since "this log of transactions within an identification system becomes a map of a human's life," controlling that limit was crucial.[96] More importantly, the Court directed the Indian government to urgently "adopt and enforce a robust data protection law."[97] Justice Chandrachud emphasized the importance of this instruction in his dissent, saying "unless the law mandates an effective data protection framework, the quest for liberty and dignity would be as ephemeral as the wind."[98]

While the Court hoped these restrictions and mandates would provide some relief to those concerned for their privacy, their convictions may be more idealistic. As reported by *The Washington Post*:

> During the final hearings in early 2018, India's Supreme Court granted temporary reprieve from the compulsory linking of Aadhaar for basic services. But the government appears to be implementing the directive only half-heartedly. Both the state and businesses alike continue to push residents to submit Aadhaar numbers for many services.[99]

Moreover, concerns regarding the mandatory nature of the system generally, the data security system, the laws in place, the amount of biometric data, and the additional information collected, are still valid, as the Court has not robustly addressed these issues. As such, with domestic legal remedies essentially exhausted, Indian citizens need to turn to India's international obligations for recourse to ensure that their fundamental right to privacy is protected.

---

93 *Id.*
94 *Id.*
95 *Id.*
96 *Initial Analysis of Indian Supreme Court Decision on Aadhaar, supra* note 9.
97 *Id.*
98 *Id.*
99 Khera, *supra* note 3.

III. INTERNATIONAL RIGHT TO PRIVACY ESTABLISHED UNDER THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

A. Right to Privacy

A large set of international declarations and treaties exist to provide universal basic human rights protection to all individuals.[100] The ICCPR is one of the most important global human rights treaties, as it is a binding treaty that has been ratified by 172 countries.[101] India signed the ICCPR on April 10, 1979.[102] The ICCPR codifies numerous individual rights, including an individual's right to privacy.[103] Article 17 of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation."[104]

Scholars have regularly noted that the scope of the protected privacy right, remains ambiguous.[105] The text of the provision and the negotiating history does not provide clarity regarding the bounds of the individual right, nor do they assist states with the understanding of the exceptions to this right.[106] As a result, the Human Rights Committee (HRC), which is the governing body of the ICCPR, issued General Comment 16, to help parties comprehend their obligations under Article 17 of the treaty.[107] General Comments typically serve this exact purpose: they "elaborate on, and develop, open-textured rights language; they collate jurisprudence on a right; and they clarify the

---

100 *International Rights*, U.N. HUMAN RIGHTS, https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx (last visited Sept. 11, 2019) (The Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights, form the International Bill of Rights).

101 G.A. Res. 2200A (XXI), Int'l Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

102 Uppaluri & Shivanagowda, *supra* note 66, at 39.

103 G.A. Res. 2200A (XXI), Int'l Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

104 *Id.*

105 Frédéric Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 351 (2017).

106 *Id.*

107 *See* AM. CIVIL LIBERTIES UNION, PRIVACY RIGHTS IN THE DIGITAL AGE 7 (Mar. 2014), https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf.

application of a right to specific contexts."[108] They further "provide a framework that allows State Parties to ensure their compliance with protected rights."[109] However, while General Comments serve a regulatory function, they are not legally binding on state parties.[110] They are not considered amendments or additional provisions to the original treaty, but rather they serve as purely "highly persuasive" guides to the interpretation of the clause at issue.[111]

First, Paragraph 8 of General Comment 16 informs states of the scope of the right by highlighting particular activities that are considered private.[112] This includes correspondence, home life, and physical interaction.[113] However, the right to privacy can also be applied in other scenarios than those explicitly stated, as "the HRC and other experts have recognized that [the concept of 'privacy'] encompasses rights beyond those listed."[114] Scholars have suggested that "privacy protection extends to any personal information to which one would develop a reasonable expectation of freedom of intrusion."[115] "Reasonable expectation" is defensible where the "conduct is substantively personal," and usually occurs in a "non-public space" or "carried on one's person."[116]

General Comment 16 notes that the primary responsibility of ensuring the protection of this right belongs with state legislatures.[117] This essentially means that the domestic laws of the State Parties need to be written in compliance with Article 17 of the ICCPR. In order to provide direction on what "compliance" entails, General Comment 16 explains the meaning of "arbitrary and unlawful interference."[118] "Unlawful" means "no interference that can take place except in cases envisaged by the law," and "arbitrary" means "even interference

---

108 *Id.*

109 *Id.*

110 *Id.*

111 *Id.*

112 UNHRC, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (Apr. 8, 1988), https://www.refworld.org/docid/453883f922.html.

113 *Id.*

114 AM. CIVIL LIBERTIES UNION, *supra* note 107, at 9.

115 Sourgens, *supra* note 105.

116 *Id.*

117 UNHRC, *supra* note 112.

118 *Id.*

provided by the law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable under the particular circumstances."[119] Therefore, if a state action encroaching on an individual's right to privacy is both a "lawful and nonarbitrary interference," it is valid.[120] Hence, "lawful and nonarbitrary interferences" serve as limitations on an individual's right to privacy.[121]

Even though the General Comment provides definitions of permissible interferences regarding the right to privacy, the definitions applicability to actual scenarios, proves to be challenging.[122] Hence, states look to jurisprudence and scholarship for further insight.[123] Foremost, the HRC defines "interference" as "any measure that either directly or indirectly infringes on an individual's privacy interests."[124] Next, practice by the HRC and adjudication of European and American cases has led to the development of a four-part test for "lawfulness."[125] The "lawfulness" test is fulfilled by satisfying the following four prongs: the interference has to be (1) "consistent with the provision, aims, and objectives of the Covenant;" (2) "pursuant to domestic and international law;" (3) "accessible and foreseeable;" and (4) "precise, specific and clearly defined."[126] Additionally, even if an interference satisfies the "lawfulness" aspect, it needs to further comply with the "non-arbitrary" test, which has further developed into a proportionality test.[127] For an interference to be "non-arbitrary," the interference "must pursue a legitimate aim," "have a rational connection to that aim," "minimally impair the right to privacy," and "strike a fair balance between pursuit of the aim and limitation of the right."[128] This proportionality assessment has developed over time through case law, in addition to being acknowledged by various United Nations experts, including the HRC.[129] Consequently, if an interference satisfies the

119 *Id.*
120 AM. CIVIL LIBERTIES UNION, *supra* note 107, at 19.
121 *Id.*
122 Sourgens, *supra* note 105.
123 *Id.*
124 AM. CIVIL LIBERTIES UNION, *supra* note 107, at 19.
125 *Id.* at 20.
126 *Id.*
127 *Id.* at 23.
128 *Id.*
129 *Id.*

"lawfulness" test, but is proven to be unreasonable by the latter test, it is unlawful.[130]

In summary, the international right to privacy requires states to protect an individual's correspondence, home life, physical interaction, and "any personal information to which one would develop a reasonable expectation of freedom of intrusion," regardless of the individual's nationality, if they are subjected to the jurisdiction of the nation.[131] However, there are limitations to the protection of this right, as states are able to interfere with it, if the interference satisfies both the "lawfulness" test, and the "nonarbitrary" test.[132]

B. Privacy in a Digital Age

The international right to privacy, which was first drafted in 1966 and codified in the ICCPR, has been in force since 1976.[133] Clarifications of its implementation provided in General Comment 16 were also drafted and presented numerous years ago in 1988.[134] Today, many questions and concerns have been raised regarding the application of this right in an age of new technologies.[135]

Over the past few decades, technology has greatly evolved and provided the world with widely disseminated innovations that were either non-existent or limited in scope during the formation of the Covenant.[136] In response to our modern age, the United Nations General Assembly adopted a resolution titled "The Right to Privacy in the Digital Age" in 2013.[137] The resolution emphasizes that the unlawful or arbitrary collection of personal data, violates privacy rights, as they are highly intrusive acts.[138] In particular, it notes that the General Assembly is "deeply concerned" with state practices of collection of mass amounts of personal data, as they may have a negative impact on the "exercise and enjoyment of human rights."[139] The drafters of General Comment 16 anticipated this development, as evidenced by the

130 AM.CIVIL LIBERTIES UNION, *supra* note 107, at 13; Sourgens, *supra* note 105.
131 Sourgens, *supra* note 105.
132 AM. CIVIL LIBERTIES UNION, *supra* note 107, at 23.
133 *Id.* at 3.
134 UNHRC, *supra* note 112.
135 AM.CIVIL LIBERTIES UNION, *supra* note 107, at 3.
136 *Id.*
137 G.A. Res. A/RES/68/167 (Jan. 21, 2014).
138 *Id.*
139 *Id.*

inclusion of Clause 10, which states that safeguards to protect privacy need to be implemented when gathering personal information.[140] The notion that the collection of personal information infringes upon the right to privacy has been bolstered over the years, as the HRC and the European Court have often stated the same.[141]

In its sessions, the HRC has determined that the mass collection of information "may infringe on privacy, and that mere collection and storage of data—even data that is publicly accessible—may constitute an 'interference' that is subject to the constraints imposed by Article 17."[142] Considering the matter further, the European Court has continuously stated that the right to privacy affords individuals the right to protect their personal data.[143] The European Court defines personal data as "not just data that can be used for personal identification purposes, but any 'data relating to the private life of an individual.'"[144] In *Malone v. United Kingdom*, the European Court stated that "the individual is more and more vulnerable as a result of modern technology . . . Man in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality."[145] Consequently, in their practices the European Court and European Union Advocate General have consistently opined that "blanket and indiscriminate" retention of personal information is a "disproportionate interference with the right to privacy."[146]

Many scholars have echoed similar conclusions in their research. They have additionally noted that "personal information" includes medical information, financial information, information on personal affairs, and demographic information.[147] The privacy right associated with personal information is that to control the information,[148] to "avoid unwilling exposure of personal information, or to be able to provide selective access to oneself," and a "desire for freedom from

---

140 *Id.*; UNHRC, *supra* note 112.

141 AM. CIVIL LIBERTIES UNION, *supra* note 107.

142 *Id.* at 4.

143 *Id.* at 15.

144 *Id.*

145 *Id.*

146 *Id.* at 27.

147 Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63, 64 (2006).

148 Lillian R. BeVier, *Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 459 (1995).

observation."[149] This is because individuals desire to maintain their anonymity and personal autonomy by remaining free from social pressures.[150] However, given the massive amounts of information possessed and the nature in which it is collected, personal data provides full profiles of individuals.[151] Therefore, when government entities collect personal information from citizens, a very common practice around the globe, they have a duty to protect the privacy of such information.[152]

However, while the collection of personal information is the norm for most effective government systems, national identification cards that would streamline many government processes are rare, as they are seen as the "most visible component of a massive verification and tracking infrastructure."[153] Since national identification cards are accompanied by databases that "verify and monitor the movements of millions of individuals," an immensely invulnerable security system would be required to prevent any infiltration or glitch in the system.[154] This idealistic goal is simply impossible, as the mechanics of such a system would still not protect regular citizens against a devious government employee or highly skilled digital terrorist.[155] Moreover, governments should only collect the data necessary to serve their prescribed functions, and individuals should be notified as to how their information is being used.[156]

To account for all of the changes that have occurred since 1988, the American Civil Liberties Union (ACLU) recommends that a new General Comment be issued.[157] The ACLU writes:

> a new General Comment is required to clarify the use of the terms "privacy," "home," and "correspondence" as used in Article 17 so that they more accurately describe their

149 Daniel E. Newman, *European Union and United States Personal Information Privacy, and Human Philosophy – Is There a Match?,* 22 TEMP. INT'L & COMP. L.J. 307, 311, 314 (2008).

150 *Id*. at 312-15.

151 Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 304 (2003).

152 Barber, *supra* note 147, at 63-64.

153 *Id.* at 106.

154 *Id.* at 107-08.

155 *Id.*

156 *Id.* at 113.

157 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 4.

> meaning in a society in which billions of people worldwide increasingly communicate and otherwise conduct their personal and working lives online.[158]

More importantly, the ACLU also states that the General Comment should include a modern interpretation of "interference," as with new technologies, states are now able to infringe upon citizens privacy on a much larger scale.[159]

As such, based on the "nonarbitrary" requirement, recent jurisprudence, and scholarship, the ACLU proposes that the new General Comment, should state that data collection practices must always ensure that minimal safeguards are in place to protect privacy interests, and that mass storage of personal data essentially always violates Article 17.[160] The ACLU also requests that the new comment provide guidelines for what comprises "minimal safeguards."[161]

IV. INDIA'S AADHAAR CARD USAGE – VIOLATION OF ARTICLE 17 OF THE ICCPR?

In order to analyze whether a particular measure legally interferes with an individual's right to privacy, a synthesis of the rules is warranted. General Comment 16 provides that any personal information to which one would develop a reasonable expectation of freedom of intrusion is subject to Article 17 of the ICCPR, and compliance with the right of privacy requires that state interference with the right to privacy be both "lawful" and "nonarbitrary."[162] The HRC outlined a four-part test for "lawfulness" and a proportionality test for "nonarbitrary" that guides the analysis.[163] Moreover, these tests apply to the state collection of personal data. For example, in "The Right to Privacy in the Digital Age," the General Assembly resolution states that unlawful and arbitrary collection of personal data, violates the right to privacy.[164] An interpretation of the resolution provides that any limitation must:

---

158 *Id.*
159 *Id.* at 12.
160 *Id.* at 25-27.
161 *Id.* at 28.
162 Sourgens, *supra* note 105.
163 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 20.
164 G.A. Res. A/RES/68/167 (Jan. 21, 2014).

> be provided by law (meaning the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances); be necessary for reaching a legitimate aim; and be proportionate (meaning the surveillance activity must be in proportion to the aim and the least intrusive option available).[165]

As such, this serves as the initial framework for determining whether India, through its Aadhaar Card system, has violated Article 17 of the ICCPR.

As previously stated, in order to receive an Aadhaar Card, individuals must submit biometric data, such as fingerprints and iris scans, along with demographic information, such as their date of birth and gender.[166] According to scholarly interpretations of General Comment 16, such data qualifies as personal information as it is about one's physical body.[167] Moreover, information tied to the Aadhaar database, such as marital status, tax information, and government benefits, is also considered to be personal information in the realm of data privacy.[168] Hence, the information collected and stored in relation to the Aadhaar Card is subject to an individual's right to privacy.

To determine the Aadhaar Card system's "lawfulness," the four-prong test provides that the interference has to be "consistent with the provision, aims, and objectives of the Covenant," "pursuant to domestic and international law," "accessible and foreseeable," and "precise, specific and clearly defined."[169] The analysis here is relatively straightforward, as the Indian government has passed the Aadhaar Act and Income Tax Act to provide a set of legislations for the Aadhaar Card system that have been deemed valid and constitutional by the Indian Supreme Court.[170] As such, the collection of information is well defined, foreseeable, and pursuant to domestic Indian law. The Indian Supreme Court has also determined that the Aadhaar Card system is not in violation of an individual's right to privacy and is therefore

165 *Id.* at 8.
166 Chaturvedi, *supra* note 3.
167 Sourgens, *supra* note 105.
168 Barber, *supra* note 147, at 64.
169 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 20.
170 Chaturvedi, *supra* note 3.

domestically consistent with the aims of the ICCPR. However, to fully comply with the provision, the system would also need to satisfy the proportionality test for arbitrariness. The proportionality test for arbitrariness states that the interference "must pursue a legitimate aim," "have a rational connection to that aim," "minimally impair the right to privacy," and "strike a fair balance between pursuit of the aim and limitation of the right."[171]

The initial phase of the Aadhaar system satisfies the first prong of this test, as there are legitimate governmental purposes for implementing this system. As mentioned previously, the system has been adopted to account for India's growing population and to provide benefits to all citizens by diminishing identity theft.[172] However, the government has not provided any reasoning for the additions that have come later, such as having to present the card for marriage certificates and income tax filings. An appropriate justification is needed for the continued expansion of the Aadhaar Card, as the purpose provided at the onset of the program, to have a less reproducible identification card system to better provide benefits to lower-income individuals, is inadequate.[173] One argument is that the later developments have the same purpose as the original goal, since linking more information to the Aadhaar system means that the government has an easier task of tracking and providing for citizens. However, a legitimate purpose for the later developments has not been provided by the government.[174]

The second part to the proportionality test demands that the Aadhaar system exist as a rationally related means toward the government's goal of accounting for its population and to more efficiently provide benefits for all of its citizens.[175] As such, the unique identification number, combined with the biometric and demographic information linked to the card, does help the government to better provide for its citizens, as it reduces the chances of identity theft and streamlines the process of providing various benefits.[176] Furthermore, if it is assumed that the later additions to the Aadhaar Card are for the same purposes as its initial proposal, consolidating personal information

171 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 23.

172 Chaturvedi, *supra* note 3; Bhatia, *supra* note 4.

173 *Id.*

174 *Id.*

175 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 23; Chaturvedi, *supra* note 3; Bhatia, *supra* note 4.

176 Chaturvedi, *supra* note 3; Bhatia, *supra* note 4.

from distinct divisions into one central database, this reasoning would serve as a rational means to help the government better account for its very large population.

Third, an inquiry as to whether the Aadhaar system "minimally impairs the right to privacy" is needed.[177] While the Indian Supreme Court has found that the information collected in the Aadhaar system is insignificant, and therefore "minimally impairs the right to privacy," scholars around the world would most likely disagree. Scholars have stated that when a government collects and stores personal information, at minimum it needs to provide robust and effective data security systems and laws.[178] As outlined previously, the Aadhaar central database has been subject to many security breaches, and it is vulnerable to more in the future, as its data security infrastructure is easily susceptible to being penetrated.[179] Furthermore, in its 2018 opinion, the Indian Supreme Court ordered the government to develop more robust data security laws to better protect programs such as the Aadhaar centralized database.[180] This indicates that for the nine years, since the implementation of the Aadhaar Card program until the Supreme Court ruling, inadequate protections have remained in place to protect deeply private information. An extremely large amount of personal data has been susceptible to theft and dissemination.[181] This is gravely damaging to an individual's desire for privacy, as individuals have no control over who can see their data or how they are using it, which affects the basic desire for anonymity and autonomy.[182] According to Grayson Barber, this is the very reason many government systems have not implemented national identification systems.[183]

During the process of registering for the card, the Aadhaar Card system also significantly impairs the right to privacy. As previously outlined, the Aadhaar system requires individuals to submit their fingerprints and iris scans, along with additional demographic information.[184] This information ensures that the card exclusively belongs to one individual, as iris and fingerprint patterns are completely unique

177 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 23.
178 *See* Barber, *supra* note 147, at 64.
179 Khaira, *supra* note 41.
180 Chaturvedi, *supra* note 3.
181 *Id*; McKenna, *supra* note 3, at 752.
182 *Id*; Newman, *supra* note 150, at 311, 314.
183 Barber, *supra* note 147, at 64.
184 Chaturvedi, *supra* note 3.

to each human being.[185] However, the mandatory collection of this information also implicates an individual's desire for anonymity, as the government can trace the card to that one specific citizen. While this is in line with the government's purpose behind creating this system, the mechanics of the system go beyond minimally impairing an individual's right to privacy.

Finally, the proportionality aspect of the "nonarbitrary" test needs to be satisfied, which states that the Aadhaar Card system needs to "strike a fair balance between pursuit of the aim and the limitation of the right."[186] This analysis is informed by the European Court jurisprudence, in which it recently stated that "blanket and indiscriminate" retention of personal information is a "disproportionate interference with the right to privacy."[187] This is in line with the ACLU's recommendations, which state that the mass storage of information always violates Article 17.[188] Furthermore, scholars have opined that governments should only collect the data that is necessary to carry out their prescribed functions.[189]

Viewed through this lens, the Aadhaar Card is a disproportionate invasion of one's right to privacy. It therefore makes it mandatory for all citizens of India to obtain one and does not differentiate between citizens who many need this program against those who may not. Initially, when the program was run on a voluntary basis, the Aadhaar Card would have satisfied this analysis as only those who were in need of such an identification card could opt in to receive the benefits derived from doing so.[190] However, with a blanket requirement for all Indian citizens, the government does not just collect information from lower income individuals who may need this system, but does so from those who are not the intended targets of the program. As Justice Chandrachud opined in his dissenting opinion, the mandatory nature of the Aadhaar system makes it "impossible for a citizen to live in contemporary India without Aadhaar," which is overly broad.[191]

---

185 Sandee LaMotte, *The Other 'Fingerprints' You Don't Know About*, CNN (Dec. 4, 2015), https://www.cnn.com/2015/12/04/health/unique-body-parts/index.html.

186 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 23.

187 *Id.* at 27.

188 *Id.* at 25-27.

189 Barber, *supra* note 147, at 113.

190 Chaturvedi, *supra* note 3; Bhatia, *supra* note 4.

191 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

In addition to the mandatory nature of the program, the system is disproportionate to its aims because it collects and stores more information than is necessary to fulfill its goals. In order to account for its citizens, the government does not need two types of biometric information, both iris and fingerprint scans, to do so. Since these are both unique aspects of an individual, the government should only require one, to trace the identification card back to that specific person. It does not need to collect both. Furthermore, the later additions of using the unique identification number to file tax information and certify marriages, are also unnecessary for carrying out the purpose of accounting for citizens, and instead serves the desire for administrative efficiency. Connecting this information to the Aadhaar Card greatly impairs on the right to privacy, as the government is able to construct full profiles of individuals if it chooses to do so.[192] This excessive addition implicates the human desire for autonomy and anonymity, disproportionately interfering with Article 17.

This conclusion is counter to that of the Indian Supreme Court, which conducted a similar proportionality analysis when reaching the conclusion that the Aadhaar Card program did not implicate an individual's right to privacy.[193] That is because the Indian Supreme Court determined that minimal information was collected in order to achieve the government's goals, which would not be possible without the particular system in place.[194] As such, it deemed the means to be rationally related and narrowly tailored to the government's objective.[195] However, that is not the case given the nature of the information collected, the amount of information collected, and based on who the information is collected from.

Thus, while the Aadhaar Card program may be in lawful interference with an individual's right to privacy, it is still arbitrary, as it is a disproportionate violation. As such, India is not in compliance with the Article 17 of the ICCPR, since General Comment 16 states that an interference with the right needs to be both "lawful" and "nonarbitrary" to continue to be in obedience.[196]

---

192 McKenna, *supra* note 3, at 753.

193 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

194 *Id.*

195 *Id.*

196 Sourgens, *supra* note 105.

V. INDIA'S COMPLIANCE WITH ARTICLE 17 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

India's compliance with Article 17 of the ICCPR is paramount, as it is an international treaty that India is a party to.[197] This means that India has an obligation to fulfill its commitment under international law.[198] The General Assembly resolution, titled "The Right to Privacy in the Digital Age," also reminds states that "while concerns about public security may justify the gathering of certain sensitive information, States must ensure full compliance with their obligations under international human rights law."[199] As such, India needs to change the Aadhaar Card system so that it is in compliance with its obligation under Article 17 of the ICCPR.

A. Changes to the Aadhaar Card Program

The most important amendment to the Aadhaar Card program has to be in relation to its data security. First and foremost, a robust and impenetrable data security system needs to be designed and implemented in order to protect Indian citizens' personal information. If such technology does not exist, perhaps the best way to ensure security would be to store data on multiple databases instead of on one central database. Furthermore, data privacy laws need to be swiftly passed in Parliament so that there are clear legal obligations to protect information. If the government is going to continue to collect personal information, it must ensure that the data it is demanding from individuals is heavily guarded and astoundingly secure. This will help regulate who has access to each individual's personal information and lower the impairment of privacy under the third prong of the "arbitrary" test.

Second, the Aadhaar Card system would be equally as effective if it collected and linked less data to the one unique identification number. In order to fulfill its purpose, the Aadhaar Card needs to only be connected to one exclusive marker—an individual's fingerprint. As previously mentioned, since fingerprints and iris patterns are unique

197 G.A. Res. 2200A (XXI), Int'l Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

198 Paolo G. Carozza, *Subsidiarity as a Structural Principle of International Human Rights Law*, 97 AM. J. INT'L. L. 38, 46 (2003).

199 G.A. Res. A/RES/68/17 (Jan. 21, 2014).

to each individual, the card needs only one of them to ensure that the card is not susceptible to theft or reproduction. Moreover, since tax information and marital status are both unnecessary to achieve the desire of accounting for its citizens, the Indian government must stop the collection of these data points and delete them off the current system. If proven otherwise, the data storage system would still need to be changed in order to keep the biometric and demographic data sets separate from the tax and marital information. This would safeguard citizens from government profiling and help India better "strike a fair balance between pursuit of the aim and limitation of the right."[200]

Finally, the mandatory nature of the Aadhaar Card needs to be revoked and the program should be reverted back to when it was conducted on a voluntary basis. Those who determine that participation in the program would be beneficial to them will opt in and reap the rewards of doing so. Through this scheme, the government will still be able to efficiently provide services to those who are disadvantaged by the previous administrative system. Furthermore, the previous identification card infrastructure could remain in place, allowing the government to still account for all of its citizens through a combination of both systems. This arrangement allows for individuals to make choices while still in pursuit of the government's aims.

If the Indian government adopts these changes to the Aadhaar Card program, the program will fare better under the "nonarbitrary" test and bring itself in compliance with its obligation under Article 17 of the ICCPR.

B. Ensuring India's Compliance with ICCPR Article 17

Convincing the Indian government to implement the proposed changes to the Aadhaar Card program will be a challenge, as its only obligation is to comply with Article 17 of the ICCPR, which simply states "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation."[201] India could make a claim that the Aadhaar Card program is both lawful and nonarbitrary, since the Indian Supreme Court has ruled identically, and therefore is in compliance with Article 17. Furthermore, India could state that it has not

200 AM. CIVIL LIBERTIES UNION, *supra* note 107, at 23.

201 G.A. Res. 2200A (XXI), Int'l Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

made an international commitment to any of the further clarifications, and thus, does not have to comply, if it does not choose to do so.

As stated above, many consider Article 17 to be very ambiguous and that it relies on tests and recommendations provided by authorities outside of the actual treaty.[202] Clarifications on "unlawful" and "arbitrary" are outlined in General Comment 16, with tests provided by the HRC and European Court, and applications of Article 17 in the digital age, articulated in a General Assembly resolution, as well as in insightful scholarship.[203] However, these authorities are not binding on India – they hold minimal legal power against the country.[204] Furthermore, while some parties to the ICCPR further ratified Optional Protocol I, which allows individuals to file direct complaints against their nations for violation of a provision in the ICCPR, India has not done so.[205] As such, the political process would need to be utilized to ensure that the Indian government protects Indian citizens' right to privacy, a process which would present numerous challenges on its own. Hence, the likelihood of India making changes to its Aadhaar Card program on account of this international obligation are low, leaving Indian citizens with minimal recourse through this route.

VI. CONCLUSION

India's national identification card system, the Aadhaar Card, presents issues of violations of the right to privacy.[206] Under the Aadhaar Card program, a great deal of personal information, beyond what is necessary for the government's expressed goals, is collected from citizens and stored by the government.[207] As such, citizens are concerned with the security and usage of their data.[208] In response to these concerns, the Indian Supreme Court adjudicated on whether the Aadhaar Card was a violation of India's constitutional right to privacy, and found that the Aadhaar Card program is largely in compliance with the right.[209] Therefore, this note looks to an international human

---

202 Sourgens, *supra* note 105.

203 *See* discussion *infra* Part III, Subsection B.

204 AMERICAN CIVIL LIBERTIES UNION, *supra* note 107, at 6-7.

205 Uppaluri & Shivanagowda, *supra* note 66, at 39.

206 Chaturvedi, *supra* note 3.

207 *Id.*

208 *Id.*; Bhatia, *supra* note 4; *Aadhaar Verdict: Big Data Meets Big Brother*, *supra* note 30.

209 *Initial Analysis of Indian Supreme Court Decision on Aadhaar*, *supra* note 9.

rights treaty, specifically the ICCPR, as another avenue of recourse for Indian citizens. The main inquiry was to determine whether the Aadhaar Card complies with India's binding treaty obligation under international law.

In order to conduct this analysis, supplemental documents were used to determine the standard under the ICCPR in this modern age. The study shows that the program is an arbitrary interference with Indian citizens' right to privacy and recommends specific changes to the national identification card system. However, due to the principles of international law, there are no legal enforcement mechanisms to ensure India complies with these changes. As such, the Indian people need to look to other means to ensure their fundamental right to privacy is protected.